

MODUL · BENACHRICHTIGUNGEN

Modul Benachrichtigungen & E-Mail-Integration

In-App-Glocke, E-Mail-Versand und -Eingang, Präferenzen

Produktversion 2026.08.19 · Handbuch-Revision 1.0

Stand 19.08.2026 · Plattform .NET 10 / Windows Server

ID-31 Benachrichtigungen

Modul Benachrichtigungen & E-Mail-Integration

Ein Ticketsystem lebt davon, dass die Beteiligten mitbekommen, wenn etwas passiert. Wird mir ein Ticket zugewiesen, wartet eine Genehmigung auf mich, hat der Melder geantwortet? Müsste man dafür ständig selbst nachsehen, ginge der halbe Nutzen verloren, und Wichtiges bliebe liegen.

Dieses Modul sorgt für den Informationsfluss in beide Richtungen. Nach außen meldet es Ereignisse aktiv – über die Glocke in der Anwendung und per E-Mail, wobei jeder selbst einstellen kann, worüber er informiert werden möchte. Nach innen nimmt es E-Mails entgegen: Antwortet ein Melder auf eine Benachrichtigung, ordnet Ordavis Plattform die Nachricht automatisch dem richtigen Ticket zu. So bleibt die Kommunikation an einem Ort, statt sich über verstreute Postfächer zu verteilen.

INHALT

- 1 In-App-Benachrichtigungen (Glocke)
- 2 E-Mail-Versand (SMTP)
 - 2.1 E-Mail-Signaturen
- 3 E-Mail-Eingang (IMAP)
 - 3.1 Was mit der Nachricht danach geschieht
- 4 Sichere E-Mail (OAuth2 & TLS)
- 5 Benachrichtigungs-Präferenzen
- 6 Kontakte
- 8 Messenger (Mattermost, generischer Webhook)
 - 8.1 Verbindung einrichten
 - 8.2 Zwei Ziele, die nie vertauscht werden
 - 8.3 Versand, Wiederholung und Grenzen
 - 8.4 Was der Zustand sagt — und was nicht
 - 8.5 Abgrenzung zur Alarmierung
- 7 Rollen & Rechte (Auszug)
- Verwandte Themen

1 In-App-Benachrichtigungen (Glocke)

Die **Glocke** in der Kopfzeile zeigt neue Ereignisse (zugewiesenes Ticket, Genehmigung fällig, Antwort des Melders). Über REST-Endpunkte (`GET / PATCH /api/v1/notifications`) werden sie geladen und als gelesen markiert.

2 E-Mail-Versand (SMTP)

 **Nur im Client:** *Fußbereich* ▶ *Einstellungen* ▶ *E-Mail & Benachrichtigungen* · 

`system.config.manage` — Das Portal hat keine SMTP-Einrichtung; der Versand gilt für beide Oberflächen gleichermaßen.

Benachrichtigungen und Ticket-Antworten gehen per **SMTP** hinaus. Ein interner Exchange wird über **STARTTLS** (Port 587) mit FQDN und interner Root-CA angebunden; eine **Outbox** mit **Backoff** und **Rate-Limit** sorgt für zuverlässigen Versand.

Voraussetzung: Die interne Root-CA muss im Vertrauensspeicher des Servers liegen; der Mail-Server ist ggf. nur über VPN erreichbar.

 **Pflichtreihenfolge** — der Testversand (Schritt 5) ist der einzige Beleg, dass die Angaben stimmen. Ohne ihn merken Sie den Fehler erst, wenn die erste Benachrichtigung ausbleibt – und dann merkt es niemand.

1. Öffnen Sie *Einstellungen* ▶ *E-Mail & Benachrichtigungen*.
2. Tragen Sie **Server** und **Port** ein (interner Exchange in der Regel Port 587).
3. Schalten Sie **STARTTLS** ein.
4. Hinterlegen Sie Absenderadresse und Zugangsdaten.
5. Lösen Sie den **Testversand** aus und prüfen Sie den Eingang.

 **Ergebnis:** Die Testmail kommt an. Erst dann ist der Versand eingerichtet – ein gespeichertes Formular ist kein Nachweis.

Achtung: Ein Zertifikatsfehler äußert sich nicht als Fehlermeldung beim Speichern, sondern als stehengebliebene Outbox. Prüfen Sie bei ausbleibenden Mails zuerst, ob die interne Root-CA auf dem **Server** vertraut wird – nicht auf Ihrem Arbeitsplatz.

2.1 E-Mail-Signaturen

 **Nur im Client:** *Fußbereich* ▶ *Einstellungen* ▶ *E-Mail-Signatur* ·  `ticketing.config.manage` —
Das Portal führt Textbausteine und Vorlagen, aber keine Signaturen.

Ausgehende Ticket-Mails werden zentral mit einer **Signatur** versehen – einheitlich für alle Bearbeiter und rechtssicher.

So hinterlegen Sie eine Signatur:

 **Pflichtreihenfolge** — die **Firmen-Rechtsdaten (Impressum)** liefern die Platzhalter `{{company.name}}`, `{{company.address}}` und `{{company.legal_line}}`. Sind sie leer, bleiben sie in der Vorschau leer, und die Signatur sieht fertig aus, obwohl das Impressum fehlt.

1. Pflegen Sie zuerst die **Firmen-Rechtsdaten (Impressum)** — sie stehen auf derselben Seite unterhalb der Signatur-Vorlage.
2. Öffnen Sie *Fußbereich* ▶ *Einstellungen* ▶ *E-Mail-Signatur*.
3. Schreiben Sie die **globale Standard-Signatur** mit den benötigten Platzhaltern.
4. Hinterlegen Sie bei Bedarf je Support-Kanal eine abweichende Vorlage.
5. Prüfen Sie das Ergebnis in der **Live-Vorschau** – je Kanal einzeln.

6. Speichern Sie.

- ✓ **Ergebnis:** Jede ausgehende Ticket-Mail trägt die Signatur samt vollständigem Impressum.
- **Global oder je Kanal:** Eine globale Standard-Signatur gilt für alle Support-Gruppen; je Support-Kanal lässt sich abweichend eine eigene Vorlage hinterlegen.
- **Dynamische Platzhalter:** Vorlagen enthalten Felder, die beim Versand automatisch gefüllt werden – `{{agent.first_name}}`, `{{agent.last_name}}` (aus Datenschutzgründen abgekürzt), `{{agent.title}}`, `{{ticket.id}}` sowie die Firmendaten `{{company.name}}`, `{{company.address}}` und `{{company.legal_line}}`. Unbekannte Platzhalter werden entfernt; fehlt ein Vor-/Nachname, greift der Anzeigenname.
- **Impressum an jeder Mail:** Ein rechtlich vollständiges Impressum (Firmen-Rechtsdaten) wird an jede ausgehende Mail angehängt. Die Firmendaten pflegen Sie im Abschnitt **Firmen-Rechtsdaten (Impressum)** derselben Seite.
- **Verwaltung & Vorschau:** unter **Fußbereich** ▶ **Einstellungen** ▶ **E-Mail-Signatur** – mit Live-Vorschau je Kanal.
- **Best Practice:** keine eingebetteten Bilder, keine persönlichen Kontaktdaten des Bearbeiters; der Nachname wird zum Schutz der Beschäftigten gekürzt.

Berechtigung: Signaturen und Firmen-Rechtsdaten pflegt, wer `ticketing.config.manage` besitzt.

3 E-Mail-Eingang (IMAP)

Eingehende E-Mails werden automatisch Tickets zugeordnet:

- **Betreff-/Thread-Erkennung** ordnet Antworten dem richtigen Ticket zu.
- Unbekannte Absender können automatisch als **Kontakt** angelegt werden.
- **Schutzmechanismen:** Schleifen-, Bounce- und Anhangschutz verhindern Fehlverhalten.

3.1 Was mit der Nachricht danach geschieht

Verarbeitete Nachrichten werden aus dem Postfach gelöscht. Der Inhalt liegt ab diesem Zeitpunkt am Vorgang: Betreff, Text, Absender und Anhänge – und zusätzlich die **vollständige Original-Mail mit allen Kopfzeilen** als interner Anhang. Die Nachricht im Postfach ist damit eine Zweitschrift, und ein Eingang, der sie behält, sammelt auf Dauer personenbezogene Post ohne Zweck.

Wollen Sie die Zweitschriften behalten, tragen Sie in den Postfach-Einstellungen einen **Ablage-Ordner** ein – dann werden sie dorthin verschoben statt gelöscht.

Gelöscht wird ausschließlich, was nachweislich zu einem Vorgang geworden ist:

Fall	Was geschieht
Vorgang angelegt oder Antwort zugeordnet	Original hängt am Vorgang → Nachricht wird gelöscht (oder verschoben)

Fall	Was geschieht
Verarbeitung gescheitert	Nachricht geht in den Fehlerordner und bleibt dort auffindbar
Von einem Fachmodul übernommen (z. B. Berichtsmail der Datensicherung)	bleibt als gelesen im Eingang – es entsteht ja kein Vorgang, an dem das Original hinge

Der Altbestand bleibt liegen. Nachrichten, die vor dieser Fassung verarbeitet wurden, sind als gelesen markiert; der Abruf sieht sich nur **ungelesene** an und fasst sie deshalb nie wieder an. Räumen Sie diese einmal von Hand ab. Automatisch nachzuräumen wäre riskant: Bei einer gelesenen Nachricht lässt sich nicht mehr unterscheiden, ob das System sie verarbeitet oder ob ein Mensch sie nur geöffnet hat.

4 Sichere E-Mail (OAuth2 & TLS)

Für moderne Postfächer unterstützt Ordavis Plattform **OAuth2/Device-Code**. Zusätzlich gibt es **TLS-Pinning** und **Schlüsselrotation** für den Schutz gespeicherter Zugangsdaten.

Wichtig: In lokalen Testumgebungen kann der Vault-Schlüssel von den gespeicherten Geheimnissen abweichen – dann müssen die E-Mail-Zugangsdaten neu hinterlegt werden.

5 Benachrichtigungs-Präferenzen

Benutzer steuern über **Präferenzen**, welche Ereignisse sie per In-App und/oder E-Mail erhalten (z. B. `system.update.available`). Bearbeiter werden bei relevanter Ticket-Aktivität informiert.

6 Kontakte

Ein lokales **Kontaktverzeichnis** (E-Mail-Verzeichnis) speist Absender-/Empfänger-Auflösung. Bei unbekanntem Absender erfolgt – abhängig von `contacts.manage` – eine automatische Anlage.

8 Messenger (Mattermost, generischer Webhook)

Alles, was In-App oder per E-Mail gemeldet wird, kann **zusätzlich** über einen Messenger gehen. Der Messenger ist dabei ein **dritter Kanal in derselben Schaltmatrix** (§5) und kein eigener Meldungsstrom: Der Schalter steht je Ereignis und je Person neben In-App und E-Mail.

 **Der Kanal ist ausnahmslos Opt-in.** Richtet ein Mandant eine Verbindung ein, wird noch nichts verschickt — jede Person entscheidet selbst, welche Ereignisse sie im Messenger erreichen sollen.

8.1 Verbindung einrichten

Einstellungen › E-Mail › Messenger-Verbindungen (Windows-Client) bzw. Messenger-Verbindungen (Portal). Erforderlich ist das Recht `notifications.messenger.admin`; es ist **bewusst nicht** im Postfachrecht enthalten — ein Bot-Token öffnet einen anderen Dienst als ein Postfach-Kennwort.

Anbieter	Adresse	Geheimnis	Kann
Mattermost	Serveradresse, z. B. <code>https://chat.example.org</code>	Zugangstoken eines Bot-Kontos	Direktnachricht und Kanal
Generischer Webhook	vollständige Ziel-URL	optionales Geheimnis (als Bearer-Token)	nur Kanal

Das Bot-Konto muss Mitglied der Kanäle sein, in die es schreiben soll. Für Direktnachrichten genügt das Bot-Konto selbst.

Das Geheimnis wird **verschlüsselt** abgelegt (AES-256-GCM, dasselbe Verfahren wie beim Postfach-Kennwort) und von der Schnittstelle nie im Klartext zurückgegeben — sichtbar ist nur, *ob* eines hinterlegt ist.

8.2 Zwei Ziele, die nie vertauscht werden

- **Direktnachricht** an die Person: alles Persönliche — zugewiesen, Genehmigung, Erinnerung.
- **Kanal/Raum**: Team-Ereignisse ohne persönlichen Bezug, etwa ein neues Ticket ohne Zuweisung.

Die Zuordnung *Ordavis-Benutzer* → *Messenger-Konto* läuft über die **E-Mail-Adresse**. Ist eine Person im Messenger nicht auffindbar, steht das sichtbar in der Verwaltung unter *Zuordnung der Benutzer* — und nicht nur im Protokoll: Sonst glaubt jemand, benachrichtigt zu werden, und wird es nie.

⚠ Der generische Webhook kann **keine** Direktnachricht. Er meldet das, und die Oberfläche bietet sie für ihn gar nicht erst an. Persönliche Benachrichtigungen brauchen deshalb eine Anbindung mit Direktnachricht.

8.3 Versand, Wiederholung und Grenzen

Nichts wird im Anfragepfad gesendet: Nachrichten werden **eingereicht** und von einem Job zugestellt. Ein vorübergehender Fehler (Netz, 5xx, Ratengrenze) wird mit wachsendem Abstand wiederholt (1, 2, 4, 8, 16, 32 Minuten); eine **dauerhafte** Ablehnung — archivierter Kanal, gelöschttes Konto, ungültiges Token — wird **nicht** wiederholt. Nach 20 Fehlversuchen in Folge legt sich die Verbindung still, damit ein gesperrtes Bot-Konto nicht im Minutentakt angerufen wird.

Der Sende-Deckel *Nachrichten je Stunde* schützt nicht vor dem eigenen Versand, sondern vor der Ratengrenze des Dienstes. Wird er erreicht, wird die Nachricht **zurückgestellt** und nicht als Fehlversuch gezählt.

8.4 Was der Zustand sagt — und was nicht

Im Lagebild *Letzte Nachrichten* steht je Nachricht **angenommen**, **abgelehnt**, **wartet** oder **unbekannt**.

⚠ „Angenommen“ ist nicht „zugestellt“. Weder Mattermost noch ein Webhook liefert eine Empfangsbestätigung; die stärkste belegbare Aussage lautet, dass der Dienst die Nachricht entgegengenommen hat. „Unbekannt“ bleibt deshalb ein eigener Zustand und wird nicht zu einem grünen Haken geschönt.

⚠ Ein bestandener **Verbindungstest** belegt nur die Erreichbarkeit. Er räumt einen Versandfehler nicht weg — und beim generischen Webhook erzeugt er sichtbar eine Nachricht im Zielkanal, weil ein eingehender Webhook keinen Prüfweg ohne Nebenwirkung hat.

8.5 Abgrenzung zur Alarmierung

Der Messenger ist ein **Benachrichtigungsweg**, kein Alarmierungsweg. Läuft er — wie üblich — im selben Netz wie die Anwendung, stirbt er mit ihr; als Alarmweg wäre er damit auf derselben Stufe wie E-Mail. Eskalationsstufen, Quittungspflicht und Zustellnachweis im BCM-Sinn gehören deshalb nicht hierher.

7 Rollen & Rechte (Auszug)

Recht	Erlaubt
(kein eigenes Recht)	Die eigenen Benachrichtigungen sieht jede angemeldete Person; ein Recht wird dafür nicht geprüft.
<code>contacts.manage</code>	Kontakte verwalten
<code>system.config.manage</code>	E-Mail-Integration konfigurieren
<code>notifications.messenger.admin</code>	Messenger-Verbindungen verwalten (MSN-03)

Verwandte Themen

- ID-40 – Administrationshandbuch – SMTP und Postfach einrichten
- ID-20 – Modul Service Desk / Ticketing – welche Ticketereignisse Nachrichten auslösen
- ID-41 – Modul Identität, Benutzer & Rollen – wer als Empfänger infrage kommt
- ID-50 – Betriebshandbuch – Installation & Serverbetrieb – Zustellprobleme im Betrieb eingrenzen